EXHIBIT A

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

CHAMBERS OF
KAREN L. STROMBOM
CHIEF UNITED STATES MAGISTRATE JUDGE

U.S. COURTHOUSE
1717 PACIFIC AVENUE
TACOMA, WA 98402

(253) 882-3890

October 1, 2009

Robert Westinghouse
Assistant United States Attorney
U.S. Department of Justice
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271

Re: Warrant Requirements under *United States v. Comprehensive Drug Testing*

Dear Mr. Westinghouse:

In a letter dated September 21, 2009, you outlined your office's position regarding the application of *United States v. Comprehensive Drug Testing Inc.*, __F.3d __, 2009 WL 2605378 (9th Cir. August 26, 2009) (en banc) to warrants authorizing searches of electronically stored information. A copy of your letter was provided to the Magistrate Judges in this district. We met, discussed your office's position, and the *Comprehensive Drug Testing* decision to determine the impact and requirements of the decision.

The decision significantly affects the manner in which searches of electronically stored information may be conducted. It specifies that the "plain view" doctrine does not apply to such a search. It imposes additional requirements on the government in requesting a warrant, and on Magistrate Judges in issuing the warrants, with relation to the risk of destruction of data, the scope of the warrants, and procedures to be used in seizing and searching devices containing electronically stored information. It requires the government to provide a return certifying that the data or devices seized have been returned or destroyed.

The Magistrate Judges understand the United States disagrees with the majority decision in *Comprehensive Drug Testing* but as Judge Bea states in his dissent "the establishment of guidelines which are little more than dicta . . . are nonetheless binding precedent in this circuit." *Id.* at *24. Therefore, we are all required to follow the requirements set forth in the majority's decision.

Accordingly, attached is a two page outline entitled SEARCH WARRANT REQUIREMENTS FOR ELECTRONICALLY STORED INFORMATION which sets forth what we have concluded *Comprehensive Drug Testing Inc.* requires of the United States and Magistrate Judges for warrants seeking the seizure and search of electronically stored information. This outline has also received the approval of the district judges.

We expect that warrant applications for electronically stored information will comply with the requirements set forth in the attached outline. Additionally, we expect that any Assistant U.S. Attorney who submits a warrant application that deviates from these requirements will highlight those deviations to the Magistrate Judge at or before the time the application is submitted for approval. The Magistrate Judges in this district will either modify or reject any provision that does not comply with these requirements.

Thank you for your work on this matter. If you have any additional questions or concerns, please feel free to contact us.

Sincerely,

Karen L. Strombom

Karen L. Strombom
Chief U. S. Magistrate Judge

enc.

cc: Chief Judge Robert S. Lasnik

SEARCH WARRANT REQUIREMENTS FOR ELECTRONICALLY STORED INFORMATION

Pursuant to *United States v. Comprehensive Drug Testing, Inc.* __ F.3d __ WL 2605378 (9th Cir. 2009), search and seizure warrants of devices containing electronically stored information ("ESI") must meet the following requirements:

THE SCOPE OF WARRANT

1. The scope of the warrant shall be limited to the device(s) and ESI for which the government has shown probable cause.

2. The government shall set forth a protocol for sorting, segregating, decoding and otherwise separating seizable ESI (as defined by the warrant) from all other ESI. This protocol will include a requirement that any such segregating be done either by a reasonably reliable third party who possesses the device(s) or ESI that is the subject of the warrant (such as an internet service provider) or by specially trained computer personnel who are not involved in the investigation (hereafter "Filter Team")

3. The warrant shall disclose the actual risk of destruction of ESI for which it has probable cause, as well as prior efforts to seize the ESI in other judicial fora.

4. The government shall forswear reliance on the "plain view" doctrine for any ESI that it seeks to review in the enforcement of the warrant and agree that the Filter Team will not communicate any information outside the scope of the warrant that they learn during the segregation process, absent further approval of the court

SEIZURE PROCEDURES

1. If the ESI that is subject to seizure is held by a reasonably reliable third party, the third party shall provide to the Filter Team a forensic copy of the ESI described in the warrant.

2. Otherwise, a forensic copy of ESI shall be made on-site by the Filter Team, if it is safe and reasonable to do so. The actual device(s) containing ESI shall not be taken off-site unless it contains ESI that is unlawful to possess, e.g. child pornography, or the device(s) was used to commit a criminal offense, i.e. an instrumentality.

3. If it is unsafe or unreasonable to make a forensic copy of the ESI on-site, the device(s) described in the warrant may be taken off-site. The Filter Team shall then make a forensic copy of the contents of the device(s) off site.

SEARCH PROCEDURES AND LIMITATIONS

1. Only the Filter Team may search the device(s) or forensic copies containing ESI that is outside the scope of the warrant. The Filter Team will then segregate and extract only ESI that falls within the scope of the warrant.

2. Once segregated and extracted, the ESI that is within the scope of the warrant will be copied to separate storage media. Absent further order by the issuing judicial officer, only ESI that has been segregated and extracted to separate storage media and is within the scope of the warrant will be provided to investigative agents and the United States Attorney. The Filter Team shall not disclose ESI outside the scope of the warrant or use it as the basis to seek additional search warrants or to perform additional searches of the seized devices.

RETURN PROCEDURES

1. As soon as practicable, but in any event no later than within 60 days of seizure (absent further order of the issuing judicial officer), the government must provide the issuing judicial officer with a return containing a sworn certificate that:

   (a) certifies precisely what ESI it has obtained;
   (b) certifies what ESI it has returned;
   (c) certifies it has returned the actual device(s) seized; and
   (d) certifies it has destroyed any copy made of the ESI that is outside the scope of the warrant.

2. The government may retain ESI outside the scope of the original warrant or the device(s) seized for a longer time period only if the government makes application to the issuing judicial officer, establishing a need to retain the ESI or device(s) seized, and obtains supplemental authorization from the issuing judicial officer for continued retention.